

1 **CLAIMS**

2  
3 1. A method, implemented in a computing device, the method  
4 comprising:

5 accessing a new security policy to be implemented by a plurality of security  
6 engines of the computing device and to be used by the plurality of security engines  
7 in place of a current security policy;

8 each of the plurality of security engines processing at least a portion of the  
9 new security policy to establish new rules for operation of the security engine  
10 while the security engine continues to operate according to previous rules; and

11 switching, after each of the plurality of security engines is ready to begin  
12 using the new security policy, each of the plurality of security engines to the new  
13 rules substantially concurrently.

14  
15 2. A method as recited in claim 1, further comprising stopping the  
16 plurality of security engines from processing the at least a portion of the new  
17 security policy if one or more of the plurality of security engines indicates that the  
18 processing by the security engine failed.

19  
20 3. A method as recited in claim 1, wherein for each of the plurality of  
21 security engines, the security engine is ready to begin using the new security  
22 policy after the security engine has processed the at least a portion of the new  
23 security process and can nearly ensure that it can begin using the new rules as  
24 soon as it receives an indication to switch to the new security policy.

25

1           4.    A method as recited in claim 1, wherein the switching comprises  
2 calling, for each of the plurality of security engines, a function exposed by the  
3 security engine.

4  
5           5.    A method as recited in claim 1, wherein the switching comprises  
6 writing a value to a shared data structure.

7  
8           6.    A method as recited in claim 1, wherein the switching comprises  
9 firing an event across all of the security engines at once.

10  
11          7.    A method as recited in claim 1, wherein the plurality of security  
12 engines includes an antivirus engine.

13  
14          8.    A method as recited in claim 1, wherein the plurality of security  
15 engines includes a firewall engine.

16  
17          9.    A method as recited in claim 1, wherein the plurality of security  
18 engines includes an intrusion detection engine.

19  
20          10.   A method as recited in claim 1, wherein the plurality of security  
21 engines includes a vulnerability analysis engine.

22  
23          11.   A method as recited in claim 1, wherein the plurality of security  
24 engines includes a behavioral blocking engine.

25

1           12.    A method as recited in claim 1, wherein each of the plurality of  
2 security engines is part of a same application process.

3  
4           13.    A method as recited in claim 1, wherein the plurality of security  
5 engines includes one or more of: an antivirus engine, a firewall engine, an  
6 intrusion detection engine, a vulnerability analysis engine, and a behavioral  
7 blocking engine.

8  
9           14.    A method as recited in claim 13, wherein the switching comprises  
10 one or more of:

11           calling, for each of the plurality of security engines, a function exposed by  
12 the security engine;

13           writing a value to a shared data structure; and

14           firing an event across all of the security engines at once.

15  
16           15.    One or more computer readable media having one or more  
17 instructions that, when executed by one or more processors of a device, cause the  
18 one or more processors to:

19           obtain a new security policy for a plurality of security engines of the  
20 device;

21           notify each of the plurality of security engines of one or more rules from  
22 the new security policy; and

23           wait until each of the plurality of security engines has indicated that it is  
24 ready to begin using the new security policy; and  
25

1 after receipt of an indication that each of the plurality of security engines is  
2 ready to begin using the new security policy, instruct each of the plurality of  
3 security engines to begin using the new security policy.  
4

5 16. One or more computer readable media as recited in claim 15,  
6 wherein to instruct each of the plurality of security engines to begin using the new  
7 security policy is to send a switch indication to each of the plurality of security  
8 engines substantially concurrently.  
9

10 17. One or more computer readable media as recited in claim 16,  
11 wherein to send the switch indication is to call, for each of the plurality of security  
12 engines, a function exposed by the security engine.  
13

14 18. One or more computer readable media as recited in claim 16,  
15 wherein to send the switch indication is to write a value to a shared data structure.  
16

17 19. One or more computer readable media as recited in claim 16,  
18 wherein to send the switch indication is to fire an event across all of the security  
19 engines at once.  
20

21 20. One or more computer readable media as recited in claim 15,  
22 wherein the plurality of security engines includes one or more of: an antivirus  
23 engine, a firewall engine, an intrusion detection engine, a vulnerability analysis  
24 engine, and a behavioral blocking engine.  
25

1           21. One or more computer readable media as recited in claim 20,  
2 wherein to instruct each of the plurality of security engines to begin using the new  
3 security policy is to:

4           call, for each of the plurality of security engines, a function exposed by the  
5 security engine;

6           write a value to a shared data structure; and

7           fire an event across all of the security engines at once.

8  
9           22. One or more computer readable media as recited in claim 15,  
10 wherein the one or more instructions further cause the one or more processors to  
11 issue, in response to an indication from one of the plurality of security engines that  
12 it has failed in getting ready to begin using the new security policy, an indication  
13 to each of the plurality of security engines to ignore the new security policy.

14  
15           23. A method comprising:

16           notifying each of a plurality of security service providers in a computing  
17 device of one or more new rules;

18           waiting until each of the plurality of security service providers has  
19 indicated that it is ready to begin using the one or more new rules it was notified  
20 of; and

21           indicating, to each of the plurality of security service providers after receipt  
22 of the indications that the plurality of security service providers are ready to begin  
23 using the one or more new rules they were notified of, that the security service  
24 provider is to begin using the one or more new rules it was notified of.

25

1           **24.**    A method as recited in claim 23, wherein each of the plurality of  
2 security service providers is notified of a different set of one or more new rules.

3  
4           **25.**    A method as recited in claim 23, wherein the indicating to each of  
5 the plurality of security service providers that the security service provider is to  
6 begin using the one or more new rules comprises calling, for each of the plurality  
7 of security service providers, a function exposed by the security service provider.

8  
9           **26.**    A method as recited in claim 23, wherein the indicating to each of  
10 the plurality of security service providers that the security service provider is to  
11 begin using the one or more new rules comprises writing a value to a shared data  
12 structure.

13  
14           **27.**    A method as recited in claim 23, wherein the indicating to each of  
15 the plurality of security service providers that the security service provider is to  
16 begin using the one or more new rules comprises firing an event across all of the  
17 security service providers at once.

18  
19           **28.**    A method as recited in claim 23, wherein the plurality of security  
20 service providers includes one or more of: an antivirus engine, a firewall engine,  
21 an intrusion detection engine, a vulnerability analysis engine, and a behavioral  
22 blocking engine.

1           29.     A method as recited in claim 28, wherein the indicating to each of  
2 the plurality of security service providers that the security service provider is to  
3 begin using the one or more new rules comprises one or more of:

4           calling, for each of the plurality of security service providers, a function  
5 exposed by the security service provider;

6           writing a value to a shared data structure; and

7           firing an event across all of the security service providers at once.  
8

9           30.     A method as recited in claim 23, further comprising indicating, in  
10 response to an indication from one of the plurality of security service providers  
11 that it has failed in getting ready to begin using the one or more new rules it was  
12 notified of, to each of the plurality of security service providers to delete the one  
13 or more new rules it was notified of.  
14

15           31.     One or more computer readable media having one or more  
16 instructions that, when executed by one or more processors, causes the one or  
17 more processors to:

18           receive an indication of a new security policy to be used;

19           generate a new set of rules having associated data based on the new  
20 security policy;

21           continue to use a previous set of rules and associated data until an  
22 indication to begin using the new set of rules and associated data is identified; and

23           using, upon identifying the indication, the new set of rules and associated  
24 data.  
25

1           **32.**    One or more computer readable media as recited in claim 31,  
2 wherein the one or more instructions are part of a security engine.

3  
4           **33.**    One or more computer readable media as recited in claim 31,  
5 wherein the indication of the new security policy comprises one or more rules  
6 from which the new set of rules can be generated.

7  
8           **34.**    One or more computer readable media as recited in claim 31,  
9 wherein the indication to begin using the new set of rules and associated data is  
10 identified comprises a function exposed by the one or more instructions being  
11 invoked.

12  
13           **35.**    One or more computer readable media as recited in claim 31,  
14 wherein the indication to begin using the new set of rules and associated data is  
15 identified comprises identifying, in a shared data structure, a value indicating to  
16 begin using the new set of rules and associated data.

17  
18           **36.**    One or more computer readable media as recited in claim 31,  
19 wherein the instructions further cause the one or more processors to begin polling  
20 an event, and wherein the indication to begin using the new set of rules and  
21 associated data is identified comprises detecting that the event has been fired.



1           37. One or more computer readable media as recited in claim 31,  
2 wherein the one or more instructions comprises one of: an antivirus service  
3 provider, a firewall service provider, an intrusion detection service provider, a  
4 vulnerability analysis service provider, and a behavioral blocking service provider.

5  
6           38. One or more computer readable media as recited in claim 37,  
7 wherein the indication to begin using the new set of rules and associated data is  
8 identified comprises one or more of:

9           having a function exposed by the one or more instructions invoked;  
10          identifying, in a shared data structure, a value indicating to begin using the  
11 new set of rules and associated data; and  
12          detecting that an event being polled has been fired.

13  
14          39. One or more computer readable media as recited in claim 31,  
15 wherein the one or more instructions further cause the one or more processors to  
16 receive an indication to rollback, and in response to the indication to rollback  
17 ignore the new set of rules.

18  
19          40. A method, implemented in a security engine of a computing device,  
20 the method comprising:

21          receiving a new set of rules to be enforced;  
22          using a previous set of rules until an indication to begin using the new set  
23 of rules is received; and  
24          enforcing, in response to receipt of the indication, the new set of rules.

1           41.     A method as recited in claim 40, wherein the indication comprises  
2 having a function exposed by the security engine invoked.

3  
4           42.     A method as recited in claim 40, wherein the indication comprises  
5 identifying, in a shared data structure, a value indicating to begin using the new set  
6 of rules.

7  
8           43.     A method as recited in claim 40, wherein the indication comprises  
9 detecting that an event being polled has been fired.

10  
11          44.     A method as recited in claim 40, wherein the plurality of security  
12 engines includes one or more of: an antivirus engine, a firewall engine, an  
13 intrusion detection engine, a vulnerability analysis engine, and a behavioral  
14 blocking engine.

15  
16          45.     A method as recited in claim 44, wherein the indication comprises  
17 one or more of:

18           having a function exposed by the security engine invoked;  
19           identifying, in a shared data structure, a value indicating to begin using the  
20 new set of rules and associated data; and  
21           detecting that an event being polled has been fired.

22  
23          46.     A method as recited in claim 40, further comprising:  
24 receiving an indication to ignore the new set of rules; and  
25

1 in response to the indication to ignore the new set of rules, not enforcing  
2 the new set of rules but continuing to enforce the previous set of rules.

3  
4 **47.** A system comprising:  
5 a policy reader to obtain a new security policy to be enforced on the  
6 system;  
7 a plurality of security service providers;  
8 a rule set generator to generate, for each of the plurality of security service  
9 providers, a new set of rules to implement the new security policy;  
10 a manager to send, to all of the plurality of security service providers at  
11 substantially the same time, an indication to begin using the new set of rules; and  
12 wherein each of the plurality of security service providers continues to  
13 enforce a previous set of rules until instructed to enforce the new set of rules.

14  
15 **48.** A system as recited in claim 47, wherein the plurality of security  
16 service providers includes one or more of: an antivirus engine, a firewall engine,  
17 an intrusion detection engine, a vulnerability analysis engine, and a behavioral  
18 blocking engine.

19  
20 **49.** A system as recited in claim 48, wherein the manager is to send the  
21 indication by performing one or more of:  
22 calling, for each of the plurality of security service providers, a function  
23 exposed by the security service provider;  
24 writing a value to a shared data structure; and  
25 firing an event across all of the security service providers at once.

1  
2       **50.**     A system comprising:  
3       means for accessing a new security policy to be implemented by a plurality  
4 of security engines in the system, wherein the new security policy is to be used by  
5 the plurality of security engines in place of a current security policy;  
6       means for each of the plurality of security engines to continue to operate  
7 using the current security policy until an indication is received by each of the  
8 security engines to begin using the new security policy; and  
9       means for having each of the plurality of security engines begin using the  
10 new security policy substantially concurrently.

11  
12       **51.**     A system as recited in claim 50, wherein the means for having each  
13 of the plurality of security engines begin using the new security policy  
14 substantially concurrently comprises calling, for each of the plurality of security  
15 engines, a function exposed by the security engine.

16  
17       **52.**     A system as recited in claim 50, wherein the means for having each  
18 of the plurality of security engines begin using the new security policy  
19 substantially concurrently comprises writing a value to a shared data structure.

20  
21       **53.**     A system as recited in claim 50, wherein the means for having each  
22 of the plurality of security engines begin using the new security policy  
23 substantially concurrently comprises firing an event across all of the security  
24 engines at once.

25